PATENT ABSTRACTS OF JAPAN

(11)Publication number : 55-063150
(43)Date of publication of application : 13.05.1980

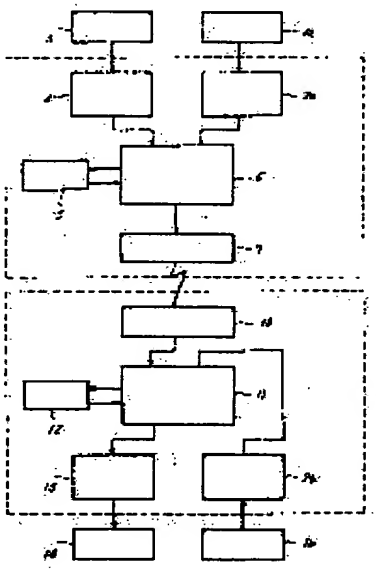
(51)Int.Cl. H04L 9/00

(21)Application number : 53-137091
(22)Date of filing : 07.11.1978

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KITAMURA KEIJI

(54) INFORMATION TRANSMISSION SYSTEM

(57)Abstract:
PURPOSE: To realize a secret information transmission system which can hold a high secrecy by giving the serial binary addition to the two output of the cipher information reader and the transmission information reader for transmission with addition of the synchronous signal and then carrying out the decoding at the reception side.
CONSTITUTION: The secret information is prepared to transmission information medium 3, and the contents of the information is read at transmission side information reader 4 to be the input of adder 6 after output in the serial binary number. While the cipher information is written into cipher information medium 1a, and this contents is read by cipher information reader 2a to be supplied to adder 6 after output in the serial binary number. Adder 6 gives the binary addition to the two output, and the synchronous signal sent from synchronous signal generator circuit 5 is added to the output to be transmitted through transmission side transmission processor 7. The transmitted information is read by reception side transmission processor 10 and then supplied to subtractor 11 in the form of the serial binary number. On the other hand, the contents prepared at docoding information medium 1b is read through decode information reader 2b and then supplied to subtractor 11 to be subtracted according to the synchronous signal sent from synchronous signal detection circuit 12. Thus the original secret information is written into reception information medium 14.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

IP-1534
2/1/31

Document 3

⑲ 日本国特許庁 (JP)　　⑪ 特許出願公開

⑫ 公開特許公報 (A)　　昭55—63150

⑤1Int. Cl.³　識別記号　庁内整理番号
H 04 L 9/00　6321—5K

⑬公開 昭和55年(1980)5月13日

発明の数 2
審査請求 未請求

(全 4 頁)

⑤4情報伝送方式

⑦1出願人 三菱電機株式会社
東京都千代田区丸の内2丁目2番3号

⑦4代理人 弁理士 葛野信一　外1名

⑦2発明者 北村桂二
鎌倉市上町屋325番地三菱電機株式会社計算機製作所内

⑦1特願 昭53—137091
⑦2出願 昭53(1978)11月7日

明　細　書

1. 発明の名称

情報伝送方式

2. 特許請求の範囲

(1) 暗号情報が書き込まれた暗号情報媒体から暗号情報を読み取り、直列の2進数で暗号を出力する暗号情報読取装置と、機密情報が書き込まれた送信情報媒体から機密情報を読み取り、直列の2進数で情報を出力する送信情報読取装置と、上記二つの出力を個々に直列2進加算し、同期信号発生回路の指令に基づいて同期信号を付加する加算器と、上記加算器の出力を外部の伝送路へ伝送情報として送信する送信側伝送処理装置とを備え、伝送すべき機密情報を暗号で変調して送信するようにしたことを特徴とする情報伝送方式。

(2) 解読情報が書き込まれた解読情報媒体から解読情報を読み取り、直列の2進数で解読情報を出力する解読情報読取装置と、外部の伝送路から受信した機密情報を含む伝送情報を直列の2進数に変換して出力する受信側伝送路処理装置と、上記二つの出力を同期信号検出回路の指令に基づいて同期をとりながら個々に直列2進減算する減算器と、上記減算器の出力を受信情報媒体に書き込む受信情報書込装置とを備え、受信側にて上記伝送情報を上記解読情報で復調して伝送された機密情報を得るようにした情報伝送方式。

3. 発明の詳細な説明

この発明は、情報伝送方式に関する。情報伝送においてしばしば高度の機密性が要求され、外部に上記情報が漏洩することを防止しなければならないことがある。この発明は、伝送系本来の機能になんらの阻止を与えることなく、高度の機密性の保持を容易に可能ならしめる情報伝送方式を提供するものである。

従来、高度の機密性を要する情報を伝送する場合、乱数による暗号化が一般的である。すなわち、情報の送信側は、伝送すべき機密情報を乱数により符号化(変調)し、この符号化され

(1)　(2)

の形式で外部の伝送路へ送信する。上記伝送情報を受信する受信側伝送路処理装置と、解読情報書込装置により完全に暗号情報と同一の解読情報が書き込まれた解読情報媒体の解読情報を読み取り直列の2進数で解読情報を出力する解読情報読取装置とをもち、上記二つの出力を同期信号検出回路の指令に基づいて同期をとりながら、個々に直列2進減算する減算器により復調して受信情報書込回路を経由して受信情報媒体に書き込むようにして、機密情報の高速、多量かつ高品質な伝送を容易に可能にし、伝送路例えば公衆回線、空中線における機密漏洩の完全防止を図るものである。

以下図によつてこの発明の実施例を説明する。第1図において(1a)は、暗号情報が書き込まれた暗号情報媒体、(1b)は解読情報が書き込まれた解読情報媒体、(2a)は暗号情報媒体(1a)の内容を読み取り直列の2進数で暗号情報を出力する暗号情報読取装置、(2b)は解読情報媒体(1b)の内容を読み取り直列

た情報をしかるべき通信手段により相手側へ送出する。一方上記の符号化された情報を受理した受信側は、あらかじめ発信側と約束した乱数に基づいて復号化(復調)して伝送されてきた機密情報を知る。

上記した従来の方式は送信側と受信側が同一の乱数情報を用意しなければならないため機密情報の伝送手段としては、機密性、伝送速度等に欠点があつた。

この発明はこのような従来方式のもつ欠点を除去するものであり、その特徴とするところは暗号情報書込装置により暗号情報が書き込まれた暗号情報媒体の暗号情報を読み取り直列の2進数で暗号情報を出力する暗号情報読取装置と、機密情報が書き込まれた送信情報媒体の機密情報を読み取り直列の2進数で情報を出力する送信情報読取装置をもち、上記二つの出力を個々に直列2進加算し同期信号発生回路の指令に基づいて同期信号を付加する加算器により変調して送信側伝送路処理装置を経由して、伝送情報

の2進数で解読情報を出力する解読情報読取装置、(3)は送信する機密情報が書き込まれた送信情報媒体、(4)は送信情報媒体(3)の内容を読み取り直列の2進数で送信情報を出力する送信情報読取装置、(5)は同期信号発生回路、(6)は同期信号発生回路(5)の指令に基づいて同期信号を付加し上記二つの出力を直列2進加算する加算器、(7)は加算器(6)の出力を外部の伝送路へ伝送情報として送信する送信側伝送処理装置、(8)は本発明に係る送信器、(9)は公衆回線、空中線で代表される伝送路であり、(10)は外部の伝送路から伝送情報を受信する受信側伝送処理装置、(11)は解読情報読取装置(2b)の出力と受信側伝送処理装置(10)の出力を直列2進減算する減算器、(12)は受信側伝送処理装置(10)の出力に含まれる同期信号を検出して起動、停止等の指令を減算器(11)に与える同期信号検出回路、(13)は減算器(11)の出力を入力して送信情報と同一の形式となつた受信情報を出力する受信情報書込装置、(14)は上記出力を記憶する受信情報媒体である。(15)は本発

明に係る受信器である。

次に第1図に示したこの発明の実施例による動作を順を追つて説明する。

高度の機密を必要とする送信情報すなわち、機密情報が送信情報媒体(3)の内容として用意される。上記媒体(3)は通常、紙テープ、紙カード、カセット磁気テープ、磁気テープ、ディスクカートリッジあるいはディスクシート等である。上記媒体(3)上に記憶された機密情報の記憶形式は上記媒体(3)自身に依存する。上記媒体(3)の内容は、送信側情報読取装置(4)によつて読み取られ、直列の2進数の形式で出力されて加算器(6)の一つの入力となる。一方、暗号情報は暗号情報が書き込まれた暗号情報媒体(1a)の内容として用意される。上記媒体(1a)は通常前記媒体(3)と同種類のものが使われる。上記媒体(1a)上に記憶された暗号情報の記憶形式は上記媒体(1a)自身に依存する。上記媒体(1a)の内容は暗号情報読取装置(2a)によつて読み取られ、直列の2進数の形式で出力

され加算器(5)のもう一つの入力となる。上記二つの出力は、加算器(4)で1ビット毎独立に2進加算される。

上記2進加算は一種の変調動作であり、送信情報が被変調信号であり、暗号情報が変調信号である。例えば、送信情報が論理"0"のとき、これに対応する乱数情報が論理"0"であれば出力は論理"0"であり、逆にこれに対応する乱数情報が論理"1"であれば出力は論理"1"である。加算器(4)の直列の2進数の出力は、送信動作起動後一定間隔毎に同期信号発生回路(5)により同期信号が付加される。上記同期信号は通常変調された上記出力と明確に区別されるものが選ばれる。例えば論理"0"を十数個連続して付加する方法がある。なお上記同期信号は、後述のとおり暗号情報の先頭に記された開始指標を基準にして付加される。加算器(4)の直列の2進数の出力は、送信側伝送処理装置(7)により該当伝送路に適合した伝送様態で送信される。

上記伝送様態とは、例えば公衆回線における

各種有線通信方式、空中線における各種無線通信方式である。

以上が送信器(A)側の動作である。

次に受信器(B)側の動作を述べる。

伝送路を経由して外部から送信されてきた伝送情報は受信側伝送処理装置(8)によつて読み取られ直列の2進数の形で出力され、減算器(9)の一つの入力となる。一方、解読情報は解読情報媒体（1b）の内容として用意される。上記媒体（1b）は、通常前記媒体(3)と同種類のものが使われる。上記媒体（1b）上に、記憶された解読情報の記憶形式は上記媒体（1b）自身に依存し、上記記憶内容は送信側の前記媒体（1a）と完全に同一である。

上記媒体（1b）の内容は解読情報読取装置（2b）によつて読み取られ直列の2進数の形式で出力され減算器(9)のもう一つの入力となる。

上記二つの出力は、減算器(9)で1ビット毎独立に2進減算される。

上記2進減算は一種の復調動作であり、受信

情報が被復調信号であり、解読情報が復調信号である。例えば、受信情報が論理"0"のとき、これに対応する解読情報が論理"0"であれば出力は論理"0"であり、逆にこれに対応する解読情報が論理"1"であれば出力は論理"1"である。同期信号検出回路(10)は、受信側伝送処理装置(8)の直列の2進数の出力中にある同期信号を検出して減算器(9)の起動動作、同期動作および停止動作をおこなう。なお、上記各種動作は、上記出力中にある同期信号と前記解読情報に記された開始指標および終了指標との比較・一致により実行される。減算器(9)の直列の2進数の出力すなわち機密情報は、受信情報書込回路(11)により受信情報媒体(12)に書き込まれる。上記媒体(12)は、通常前記送信情報媒体(3)と同種類のものが使われる。

上述のごとく、暗号情報媒体（1a）と解読情報媒体（1b）の内容は合同でなければならない。そして当然なことながら暗号情報媒体（1a）は送信側で、解読情報媒体（1b）は

受信側でそれぞれ独立にかつ完全に合同な内容で生成でき、しかもその内容は第三者に容易に解読できるものであつてはならない。

上記条件を満たすアルゴリズムには例えば「公開鍵暗号方式」がある。上記方式によれば上記媒体（1a）、（1b）の情報内容は次のように発生される。

暗号化文をC、暗号鍵をE K E、基本文をM、eとnを整数とすれば

$$C \equiv E K E(M) \equiv M^{e} \pmod{n}$$

である。ここで　$0 \leq M < n-1$、$0 \leq C \leq n-1$

である。

すなわち暗号化文Mは、適当な基本文Mを定めてe乗したのち、nで割つて剰余を求めればよい。ここで暗号化文Mは暗号情報内容および解読情報内容に相当する。

ここで、暗号情報媒体（1a）の作成方法Iを第2図に示す。第2図において、(15a)は暗号鍵、(17a)は上記アルゴリズムにより暗号情報を2進数の形式で出力する暗号情報書込装

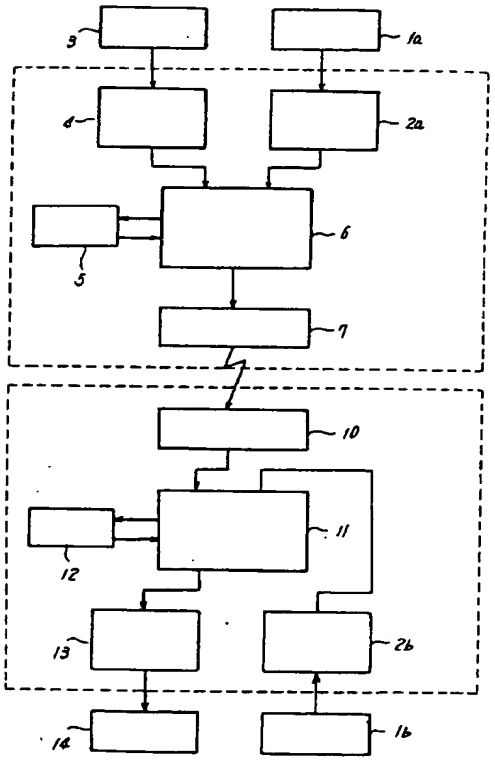
媒体の作成方法Ⅰを示す図、第3図は解読情報媒体の作成方法Ⅱを示す図である。

図において、（1a）は暗号情報媒体、（1b）は解読情報媒体、（2a）は暗号情報読取装置、（2b）は解読情報読取装置、(3)は送信情報媒体、(4)は送信情報読取装置、(5)は同期信号発生回路、(6)は加算器、(7)は送信側伝送処理装置、(8)は送信器、(9)は伝送路、(10)は受信側伝送処理装置、(11)は減算器、(12)は同期信号検出回路、(13)は受信情報書込回路、(14)は受信情報媒体、(15)は受信器、（16a）、（16b）は暗号鍵、（17a）は暗号情報書込装置、（17b）は解読情報書込装置である。

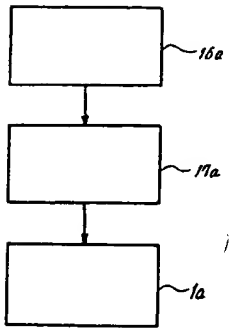
なお、図中同一あるいは相当部分には同一符号を付してある。

代理人　葛　野　信　一

第1図



第2図



第3図